Last Time: GCD.

$\gcd(a,b) = \max\{d \in \mathbb{Z} : d|a \text{ and } d|b\}$.

Prop: Let $a, b \in \mathbb{Z}$ w/ $|a| \leq |b|$ and $|b| \neq 0$.

① $\gcd(a,b) = \gcd(|a|,|b|) \geq 1$

② $\gcd(a, an+b) = \gcd(a,b)$ for all $n \in \mathbb{Z}$.

(Exercise: prove the other properties stated last time).

pf 2: Let $a, b, n \in \mathbb{Z}$ w/ not both a, b equal to 0. Let d be a common divisor of both a and b. Thus $a = dk$ and $b = dm$ for some $k, m \in \mathbb{Z}$. So $an + b = dkn + dm = d(kn+m)$ and $kn+m \in \mathbb{Z}$ by closure properties of $\mathbb{Z}$, and thus d divides $an+b$. Hence d is a common divisor of a and $an+b$. Thus $\gcd(a,b) \leq \gcd(a, an+b)$.

$\to \{d : d|a, d|b\}$
$\subseteq \{d' : d|a, d|an+b\}$

Let d be a common divisor of a and $an+b$. Thus $a = dk$ and $an+b = dm$ for some $k, m \in \mathbb{Z}$. Hence $b = dm - an = dm - dkn = d(m-kn)$ yields d divides b (because $m-kn \in \mathbb{Z}$ by closure). Hence d is a common divisor of a and b, so we obtain $\gcd(a, an+b) \leq \gcd(a,b)$.

Hence $\gcd(a, an+b) = \gcd(a,b)$ as claimed. ∎

Exercise: Give a shorter proof using "linear combination" property of divisibility...

Lem: For all $a, b \in \mathbb{Z}$ with a, b not both 0 we have $\gcd(a,b) = \gcd(b,a)$. Pf: Exercise ☒

Alg (Euclid's Algorithm): To compute $\gcd(a,b)$:

① Let $n_0 = \max\{|a|, |b|\}$ and $d_0 = \min\{|a|, |b|\}$.

② Having n_i and d_i:

Ⓐ If $d_i = 0$, output n_i.

Ⓑ If $d_i \neq 0$, use the QRT to write $n_i = d_i q_i + r_i$ (w/ $0 \leq r_i < d_i$).

Define $n_{i+1} := d_i$ and $d_{i+1} := r_i$.

Return to the beginning of step 2 (incrementing i...).

Claim: If a, b are not both 0, then the output of Euclid's Algorithm is $\gcd(a,b)$.

Ex: Compute $\gcd(5, -8)$ via Euclid's Algorithm.

Sol: $n_0 = 8$ and $d_0 = 5$

→ $8 = 5 \cdot 1 + 3$ so $n_1 := 5$ and $d_1 := 3$

$5 = 3 \cdot 1 + 2$ so $n_2 := 3$ and $d_2 := 2$

$3 = 2 \cdot 1 + 1$ so $n_3 := 2$ and $d_3 := 1$

$2 = 1 \cdot 2 + 0$ so $n_4 := 1$ and $d_4 := 0$

So we output $\gcd(5, -8) = 1$. ☒

Ex: Compute $\gcd(144, 104)$ via Euclid's Alg.

Sol: Applying Euclid's Algorithm, we obtain:

$$144 = 104 \cdot 1 + 40$$
$$104 = 40 \cdot 2 + 24$$
$$40 = 24 \cdot 1 + 16$$
$$24 = 16 \cdot 1 + 8$$
$$16 = 8 \cdot 2 + 0$$

So $\gcd(144, 104) = 8$. ∎

Q: Why does Euclid's Algorithm work?

Prop: The output of Euclid's Algorithm applied to a, b (not both zero) is precisely $\gcd(a,b)$.

(i.e. Euclid's Algorithm is "correct").

Pf: Let $a, b \in \mathbb{Z}$ with a, b not both zero.

As $\gcd(a,b) = \gcd(|a|, |b|)$, so step 1 of Euclid's Alg. preserves the gcd. For what remains, we need to show that every application of step 2 preserves gcd..

Note $n_0, d_0 \in \mathbb{N}_0$, so we proceed by strong induction on d_i ...

Base Case: If $d_i = 0$, then $\gcd(n_i, d_i) = \gcd(n_i, 0)$

Because $n_i \geq 0$, we see $\gcd(n_i, 0) = n_i$.

Induction Step: Suppose that $\gcd(n, d)$ is determined by Euclid's algorithm for all $0 \leq d \leq n$ where $d < d_i$. By our base case, we may assume $0 < d_i$. Now $n_i = d_i q_i + r_i$ for some $q_i, r_i \in \mathbb{Z}$ with $0 \leq r_i < d_i$. By the proposition from earlier today:

$$\gcd(n_i, d_i) = \gcd(d_i, n_i + d_i(-q_i)) = \gcd(d_i, r_i)$$

Thus, as $n_{i+1} = d_i$ and $d_{i+1} = r_i$, we have

$$\gcd(n_i, d_i) = \gcd(d_i, r_i) = \gcd(n_{i+1}, d_{i+1}).$$

As $0 \leq d_{i+1} < d_i$ we have by our Inductive Hypothesis that $\gcd(n, d) = \gcd(n_i, d_i) = \gcd(n_{i+1}, d_{i+1})$

Hence, Euclid's Algorithm does indeed compute $\gcd(a, b)$. ☑

Remark: When we talk about finite state machines, we will give a slightly different proof ☺.

NB: If we remember the sequence of QRT applications in Euclid's Algorithm, we can write $\gcd(a, b)$ as a $\mathbb{Z}$-linear combination of a, b.

i.e. We can prove the following:

Prop (Bezout's Theorem): Given $a, b \in \mathbb{Z}$ w/ a, b not both 0, there exist $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = as + bt$. ★

(Moreover, we may express

$\gcd(a,b) = \min\{as + bt : s,t \in \mathbb{Z} \text{ and } as + bt \in \mathbb{Z}_+\}$.)

Proof is an exercise... the "moreover" is somewhat challenging.

Ex: Write $\gcd(72, 76) = 72s + 76t$ for some $s, t \in \mathbb{Z}$.

Sol: First we apply Euclid's Algorithm:

$$76 = 72 \cdot 1 + 4 \quad \leftarrow \quad \gcd(76, 72) = 4$$
$$72 = 4 \cdot 18 + 0$$

Next, apply "back-substitution":

$$76 = 72 \cdot 1 + 4 \quad \rightsquigarrow \quad 4 = 76 - 72 \cdot 1 = 76 \cdot 1 + 72(-1).$$

Hence $4 = \gcd(76, 72) = 76 \cdot 1 + 72(-1)$. ☒

Ex: Express $\gcd(13, 34) = 13s + 34t$ for some $s, t \in \mathbb{Z}$.

Sol: First we apply Euclid's Algorithm:

$$34 = 13 \cdot 2 + \underline{8}$$
$$13 = 8 \cdot 1 + \underline{5}$$
$$8 = 5 \cdot 1 + \underline{3}$$
$$\rightarrow 5 = 3 \cdot 1 + \underline{2}$$
$$3 = \underline{2} \cdot 1 + 1$$
$$2 = 1 \cdot 2 + \underline{0}$$

$\rightsquigarrow 1 = 3 \cdot 1 + \underline{2}(-1)$

$= (34 \cdot 1 + 13(-2)) \cdot 5 + 13(-3) = 13(-13) + 34(5)$

$= (13 \cdot 1 + \underline{8}(-1)) \cdot (-3) + \underline{8} \cdot 2 = \underline{8}(5) + 13(-3)$

$= (\underline{8} \cdot 1 + \underline{5}(-1)) \cdot 2 + \underline{5}(-1) = \underline{5}(-3) + \underline{8} \cdot 2$

$= 3 \cdot 1 + (\underline{5} \cdot 1 + \underline{3}(-1))(-1) = \underline{3} \cdot 2 + \underline{5}(-1)$

Hence $1 = \gcd(13, 34) = 13(-13) + 34(5)$ ☒